CLAIMS

1. A method in a client computer for encrypting an electronic mail message, the method comprising:

receiving an indication to encrypt the electronic mail message, the electronic mail message having a recipient electronic mail address;

retrieving from a local key store a public key associated with the recipient electronic mail address;

when the public key cannot be retrieved from the local key store, retrieving from a key server the public key associated with the recipient electronic mail address; and

encrypting the electronic mail message using the retrieved public key.

2. The method of claim 1 including sending the encrypted electronic mail message to the recipient electronic mail address.

3. The method of claim 1 wherein the retrieving from the key server includes:

sending to the key server a request for the public key associated with the recipient electronic mail address; and

receiving from the key server a response including the public key associated with the recipient electronic mail address.

4. The method of claim 1 wherein when the key server does not already have a public key associated with the recipient electronic mail address, the key server associates a new public and private key pair with the recipient electronic mail address.

5. The method of claim 4 wherein the key server sends a notification electronic mail message to the recipient electronic mail address describing how to access the new private key associated with the recipient electronic mail message.

6. The method of claim 5 wherein the notification electronic mail message includes an authentication code so that a user accessing the new private key can be authenticated by presentment of the authentication code.

7. The method of claim 5 wherein the notification electronic mail message includes a link to a web site through which the new private key can be accessed.

8. The method of claim 5 wherein the new private key is an interim key.

9. The method of claim 1 including storing the public key retrieved from the key server in the local key store.

10. The method of claim 9 wherein when the public key retrieved from the key server is an interim key, suppressing the storing of the public key in the local key store.

11. The method of claim 1 including

sending to the key server a request for the public key associated with the recipient electronic mail address;

receiving from the key server a response indicating that no public key is associated with the recipient electronic mail address; and

in response to receiving the response,

sending to the key server a request that a public and private key pair be associated with the recipient electronic mail address; and

receiving from the key server a response including the public key newly associated with the recipient electronic mail address.

12. The method of claim 1 wherein the electronic mail message is to be sent by a sender and including logging the sender on to the key server.

13. The method of claim 1 including signing the electronic mail message with a private key associated with a sender of the electronic mail message.

14. The method of claim 1 wherein when the encrypted electronic mail message is received at the recipient electronic mail address, the encrypted electronic mail message is automatically decrypted using a private key associated with the recipient electronic mail address.

15. The method of claim 1 wherein when a recipient receives the encrypted electronic mail message, the decrypting of the received electronic mail message is deferred until a request to decrypt is received.

16. A method in a server computer for coordinating sending of an electronic mail message from a sender to a recipient, the method comprising:

receiving from a sender computer a request for a public key associated with a recipient electronic mail address;

associating a public and private key pair with the recipient electronic mail address;

sending to the sender computer a response that includes the public key associated with the recipient electronic mail address; and

providing the private key to the recipient

so that the electronic mail message encrypted by the sender using the public key can be decrypted by the recipient using the private key.

17. The method of claim 16 wherein the providing of the public key to the recipient includes sending a notification electronic mail message to the recipient electronic mail address.

18. The method of claim 17 wherein the notification electronic mail message includes an authentication code that is used to authenticate the recipient when the interim private key is provided to the recipient.

19. The method of claim 17 wherein the notification electronic mail message includes the private key.

20. The method of claim 16 including when a subsequent request is received from a sender computer for a public key associated with the recipient electronic mail address, sending to the sender computer the public key previously associated with the recipient electronic mail address.

21. The method of claim 16 wherein the public key is an interim key and the sender computer does not persistently store the interim public key.

22. The method of claim 16 wherein the public and private key pair is used as a permanent public and private key pair for the recipient.

23. The method of claim 16 wherein the public and private pair is used as a permanent public and private key pair for the recipient when requested by to do so by the recipient.

24. The method of claim 16 including receiving a permanent public key from the recipient and replacing the public key with the received permanent public key.

25. The method of claim 16 including generating the public and private key pair.

26. The method of claim 16 including selecting the public and private key pair from a pool of previously generated public and private key pairs.

27. The method of claim 26 including changing an electronic mail address associated with the selected public and private key pair to the recipient electronic mail address.

28. A method in a server computer for coordinating sending of an electronic mail message from a sender to a recipient, the method comprising:

receiving from a sender computer a request to send the electronic mail message to a recipient electronic mail address;

encrypting the electronic mail message with a public key associated with the recipient;

sending the encrypted electronic mail message to the recipient electronic mail address; and

sending a private key to the recipient so that the electronic mail message can be decrypted by the recipient using the sent private key.

29. The method of claim 28 wherein the sending of the private key to the recipient includes sending of a notification electronic mail message to the recipient electronic mail address.

30. The method of claim 29 wherein the notification electronic mail message includes an authentication code that is used to authenticate the recipient before sending the private key.

31. The method of claim 29 wherein the notification electronic mail message includes the private key.

32. The method of claim 28 wherein the public and private key pair is used as a permanent public and private key pair for the recipient electronic mail address.

33. The method of claim 28 wherein the public and private pair is used as a permanent public and private key pair for the recipient electronic mail address when requested by to do so by the recipient.

34. The method of claim 28 including receiving a permanent public key from the recipient and replacing the public key with the received permanent public key.

35. The method of claim 28 including generating the public and private key pair after the request is received.

36. The method of claim 28 including selecting the public and private key pair from a pool of previously generated public and private key pairs.

37. The method of claim 36 including changing an electronic mail address associated with the selected public and private pair to the recipient electronic mail address.

38. A method in a client computer for encrypting digital data, the method comprising:

receiving an indication to encrypt digital data;

retrieving from a local key store a locking key associated with a user;

when the locking key cannot be retrieved from the local key store, retrieving from a key server the locking key associated with the user; and

encrypting the digital data using the retrieved locking key.

39. The method of claim 38 wherein the user has a user identifier and the locking key is mapped to the user identifier.

40. The method of claim 39 wherein the user identifier is an electronic mail address.

41. The method of claim 39 wherein the user identifier is a key identifier associated with the locking key.

42. The method of claim 39 wherein the user identifier is a user name.

43. The method of claim 38 wherein the encrypted digital data is decrypted using an unlocking key.

44. The method of claim 38 wherein the locking key is a public key of a public and private key pair.

45. The method of claim 38 wherein the digital data is content of a file.

46. The method of claim 38 wherein the digital data is content of an electronic mail message.

47. The method of claim 38 wherein the key server receives a request for a locking key for the user, it assigns a locking and unlocking key pair to the user and provides the unlocking key to the user.

48. The method of claim 47 wherein the key server notifies the user that a locking and unlocking key pair has been assigned to the user before providing the unlocking key to the user.

49. The method of claim 48 wherein the key server provides an authentication code for authenticating the user.